Aula [24.03.2020]

Os números primos

Def Um inteiro positivo $p \in \mathbb{Z}$ é chamado **primo**, se p tem exatamente dois divisores positivos: 1 e p.

Obs. $a = 1$ não é primo (!), pois tem somente 1 divisor positivo 1.

Def.2 Um inteiro $m \in \mathbb{Z}$, $m > 1$ que não é primo, chama-se **composto**.

Exemplo: 2, 3, 5, 7 — primos
4, 6, 8, 9 — compostos.

Proposição Sejam: $p \in \mathbb{Z}$ – um primo
$a, b \in \mathbb{Z}$ – dois inteiros

(1) Se $p \nmid a \Rightarrow \text{mdc}(p, a) = 1$

(2) Se $p \mid ab \Rightarrow p \mid a$ ou $p \mid b$

Prova (1) Se $p \nmid a$, assim 1 é único divisor comum entre p e a

$\Rightarrow mdc(p, a) = 1$.

(2) Seja $p \mid ab$. Suponha que $p \nmid a$, assim pelo (1), $mdc(p, a) = 1$.

Logo $[p \mid ab,\ mdc(p,a) = 1] \Rightarrow p \mid b$.

□

Corolario 1. Se $p \mid a_1 \cdot \ldots \cdot a_n$, assim $p \mid a_k$, para algum $1 \leq k \leq n$.

Prova [p/ casa usando indução].

Corolario 2 Se $p \mid q_1 \cdot \ldots \cdot q_n$, e $p, q_1, \ldots, q_n$ primos

$\Rightarrow p = q_k$ para algum $1 \leq k \leq n$

Prova Pelo Corolario 1, $p \mid q_k$.

Como q_k é primo $\Rightarrow p = 1$ ou $p = q_k$

Como p é primo $\Rightarrow p = q_k$

□

Teorema 1 [Existem infinitos primos]

Prova Suponha que tem apenas numero finito dos primos, e sejam

$$p_1, p_2, \ldots, p_t$$ - todos eles.

Considere o numero $n = p_1 \cdot p_2 \cdot \ldots \cdot p_t + 1$

$n > p_k \Rightarrow$ assim n é composto

logo existe $1 \leq i \leq t$, com $p_i \mid n$

Mas $p_i \mid p_1 \cdot \ldots \cdot p_t$. Logo

$$p_i \mid \underbrace{n - (p_1 \cdot \ldots \cdot p_t)}_{\| \; 1}, \text{ ou } p_i \mid 1$$

Contradição, pois $p_i > 1$. □

Exercício 1 Mostre que unico primo da forma $n^3 - 1$ é 7.

Prova. Escreva $p = n^3 - 1$, Como $p = n^3 - 1 = (n-1)(n^2+n+1)$
Como p primo, assim:

$$\begin{cases} n-1=p \\ n^2+n+1=1 \end{cases} \Rightarrow \begin{cases} n=p+1 \\ n(n+1)=0 \end{cases} \Rightarrow \begin{cases} p=-1 \\ n=0 \end{cases} \text{ - impossível}$$

$$\begin{cases} p=-2 \\ n=-1 \end{cases}$$

ou

$$\begin{cases} n-1=1 \\ n^2+n+1=p \end{cases} \Rightarrow \boxed{\begin{cases} n=2 \\ p=7 \end{cases}} \quad //$$

Exercício 2 Todo inteiro da forma n^4+4, $n>1$ é composto.

Solução

$$\begin{aligned} n^4+4 &= n^4+4+4n^2-4n^2 \\ &= (n^4+4n^2+4)-4n^2 \\ &= (n^2+2)^2-(2n)^2 \\ &= (n^2+2-2n)(n^2+2+2n) \end{aligned}$$

Se $n>1 \Rightarrow (n^2+2-2n)>1$ e $(n^2+2+2n)>1$

$\Rightarrow n^4+4$ é composto. //

Teorema Fundamental da Aritmética

Teorema [TFA] Qualquer inteiro $n>1$ pode ser escrito como o produto de primos. Tais apresentação é único a menos de ordem dos primos em produto.

Prova Inteiro n é composto ou primo. Se n primo — nada p/ provar.

1ª - parte Se n é composto, considere

$$S = \{ d \in \mathbb{Z} \mid d > 0,\ d \mid n \}$$

↑ divisores positivos de "n".

Pelo (PBO) S tem elemento mínimal p_1. Obviamente p_1 é primo, (se não p_1 tem divisor $\tilde{d} \neq 1$, $\tilde{d} = p_1$, logo $\tilde{d} \mid n$ e $\tilde{d} < p_1$ Contradição.) Assim $n = p_1 \cdot n_1$, com p_1-primo e $1 < n_1 < n$. Repetindo, podemos procurar p_2 primo, com $n_1 = p_2 \cdot n_2$, e

$$n = p_1 \cdot p_2 \cdot n_2, \text{ com } 1 < n_2 < n_1$$

Repetindo, temos a sequência finita

$$n > n_1 > n_2 > \dots > 1,$$

ou seja $n = p_1 \cdot p_2 \cdot \dots \cdot p_k$ e n admite a fatorização pelos primos

2ª - parte Se $n = p_1 \cdot p_2 \cdot \dots \cdot p_r = q_1 \cdot q_2 \cdot \dots \cdot q_s$, com p_i e q_j primos com

$$p_1 \leq p_2 \leq \dots \leq p_r, \quad q_1 \leq q_2 \leq \dots \leq q_s$$

Como $p_1 \mid n = q_1 \cdots q_s$, logo (pelo Corolario 2) $p_1 = q_k$ para algum k.

Portanto $p_1 \geq q_1$. Na mesma maneira $q_1 \leq p_1$, assim $\boxed{p_1 = q_1}$, assim

$$p_2 \cdot p_3 \cdots p_r = q_2 \cdot q_3 \cdots q_s$$

Repetindo $\boxed{p_2 = q_2}$ e

$$p_3 \cdots p_r = q_3 \cdots q_s$$

Se $r < s$, vamos receber (continuando) que

$$1 = q_{r+1} \cdots q_s$$

Que é absurdo, pois $q_i > 1$. Assim $r = s$ e $p_1 = q_1$, $p_2 = q_2$, $\ldots$, $p_r = q_r$.

e q.q. 2 fatorações são iguais □

Obs. Claro que alguns primos podem acontecer mais do que 1 vez na fatoriz. Por exemplo $12 = 2 \cdot 2 \cdot 3$, ou

$$100 = 2 \cdot 2 \cdot 5 \cdot 5.$$

Assim podemos reformular o Teorema Como:

TFA: Todo inteiro $n > 1$ pode ser escrito na forma única em forma canônica:

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r},$$

onde $p_1, \ldots, p_r$ — primos

$k_1, \ldots, k_r$ — inteiros positivos

e $p_1 < p_2 < \ldots < p_r$.

// —

Exercício (p/ casa)

a) Encontre n, naturais tais que n somando com $n+1$ é primo

b) Seja p um primo > 3.
Suponha que $p+2$ primo tmb.
Mostre que $p + (p+2)$ é múltiplo de 12 //.